



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/579,884

05/17/2006

Osamu Aoki

P06,0069

5969

26574

7590

03/03/2009

SCHIFF HARDIN, LLP
PATENT DEPARTMENT
6600 SEARS TOWER
CHICAGO, IL 60606-6473

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

03/03/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/579,884	Applicant(s) AOKI ET AL.	
	Examiner MICHAEL R. VAUGHAN	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 17-29,31 and 33-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 17-29,31 and 33-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 5/17/06 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

The instant application having Application No. 10/579,884 is presented for examination by the examiner. Claims 17-29, 31, and 33-38 are pending. Claims 30 and 32 have been canceled by the currently filed amendment. Claims 1-16 were previously cancelled.

Response to Amendment

Claim Objections

Claim 17 is objected to because of the following informalities:

The term score-calculator is referred to with and without the hyphenation.

Claim 19 is objected to because “a second profile” should be “the second profile”.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 31 and 36-38 are rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, *per se*. The claim lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly not a series of steps or acts to be a process nor is there a

Art Unit: 2431

combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. It is at best, functional descriptive material *per se*. The claims lack the necessary phrasing which indicates that the program is executed by a computer and said computer determines [...] comprising. It is the intelligent computer which does the processing. Computer program can do nothing without the processing of the computer device.

Descriptive material can be characterized as either “functional descriptive material” or “nonfunctional descriptive material.” Both types of “descriptive material” are non-statutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994).

Merely claiming non-functional descriptive material, i.e., abstract ideas, stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because “[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.”).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 31 and 36-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 31, the claim now recites that a program comprises software which is defined three times. It is unclear whether these instances of software are the same. It would be clearer to not have a program, which is software, comprising software. The word instruction would be more appropriate than software. The dependent claims are likewise rejection for at least the same reason.

Response to Arguments

Applicant's arguments with respect to claims 17-29, 31, and 33-38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 17-29, 31, and 33-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCallam et al. (US 2004/0230832 A1) hereinafter McCallam, in view of Sekiguchi (USP 6,711,687).

As per claims 17, 29, and 31, McCallam teaches the limitation of “an operation-receiver for receiving instruction data for executing said operation” (page 4, paragraph 0047) as the user input manager receives user inputs and directs those inputs to the data analyzer for execution.

In addition, McCallam teaches the limitations of “a first profile-creator for creating a first profile from said instruction data related to the operation for which instruction data was received by said computer”, “a first profile-storer for storing said first profile that was created by said first profile-creator”, “a second profile-creator for identifying a user that executed said operation by said instruction data, and creating a second profile related to the operation executed by said user”, and “a second profile-storer for storing, according to user, said second profiles created by said second profile-creator” (page 6, paragraph 0066) as the detection manager contains software routines, data storage, and processing means to detect an IW attack anywhere on the LAN. Detection may be based on a number of potential activities that are monitored by the detection manager. For example, insider misuse can be detected when an authorized user performs an unauthorized, or perhaps, infrequent operation that may raise the suspicion that the authorized user's computer is being misused. In another example, user profile data may

Art Unit: 2431

be stored in a database and may be used to detect an intrusion. The user may have access to a particular database but has not accessed the database for over a year. A sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

Finally, McCallam teaches the limitation of “a score-calculator for comparing said instruction data with at least one profile that is stored in said first profile-storer or in said second profile-storer, and calculating a score for determining whether said operation is an unauthorized operation” (page 6, paragraph 0068) as the comparator may examine data at network devices and compare the data to a predefined condition and (page 6, paragraph 0069) the comparator compares the collected parameters to an established user profile that reflects normal operation of the network device.

McCallum is silent in disclosing that the first profile is compared to when said computer is not logged into a user account. Examiner interprets this limitation to be a remote access to said computer by something other than a normal user logged into the computer. This is in contrast to the second profile condition which states comparison to the instruction with that of a locally logged in user account. Therefore, Examiner makes the distinction between the first and second profile as the former being created when an outside entity attempts to initiate a process on a computer remotely, and the latter being created when a local user attempts to initiate a process on the computer locally.

McCallum teaches the second profile and comparison as indicated above. McCallum is silent in explicitly teaching the condition to which the first profile is created and compared. Sekiguchi teaches this limitation in his system when it is able to detect

Art Unit: 2431

threats posed by outside (remote) computing devices which has no user account associated with them (col. 9, lines 54-65 and col. 10, lines 1-10). Sekiguchi system creates a profile and stores security management information for comparing access between computer without user intervention. Specifically this is to protect computers which do not have to have a user logged in. This reads on the newly amended limitation of comparing instruction data with first profile when there is not user account logged in. It would have been obvious to use this type of profiling and comparing with McCallum because new types of threats could be detected and blocked. Being able to stop threats at a computer without a user logged in greatly improves the response of the system. It is obvious to combined known methods which yield predictable results. Combining McCallum and the teaching of Sekiguchi as the first type of profile would allow the system to stop illegal user attempts and remote computer attempts of access on the system.

With respect to claim 18, McCallum teaches the limitations of “a first log-data-storer for storing log data of said computer”, “a second log-data-storer for storing log data according to a user of said computer”, “wherein said first profile-creator references said first log-data-storer when creating said first profile”, and “wherein said second profile-creator references said second log-data-storer when creating said second profile” (Fig. 5E; page 6, paragraphs 0067 and 0069) as a data storage device 379 containing the user profiles 400 and trend of the performance parameters 410.

With respect to claims 19, 33, and 36, McCallum teaches the limitation of “a login-detector for executing a process for detecting whether a certain user is logged into

Art Unit: 2431

said computer; wherein when said login-detector detects that a certain user is logged in, said second profile-creator creates a second profile related to said user” (0070) as the database may store the local version of the user profile. The database may also store historical values of the computer performance parameters and the user profile.

With respect to claim 20, McCallum teaches the limitation of “said login-detector executes detection processing at specified intervals while said computer is in operation” (0079).

As per claims 21, 34, and 37, Examiner supplies the same rationale as recited in the rejection of claim 17, to incorporate as the first profile the teaching of Sekiguchi.

With respect to claim 22, McCallum teaches the limitation of “said login-detector executes detection processing at specified intervals while said computer is in operation” (0079) as the service manager that determines a periodicity of monitoring computers and other network devices for indication of intrusion and misuse.

As per claims 23, McCallum is silent in teaching a third profile-creator for creating a third profile related to an operation executed by a user that is identified as a first-time user, when the user executing said operation by said instruction data is identified as a first-time user operating said computer for the first time; and

a third profile-storer for storing third profiles that are created by said third profile-creator; wherein said *score-calculator* uses at least one profile that is stored in said third profile-storer instead of said second profile-storer to determine whether said operation is an unauthorized operation. Sekiguchi teaches these limitations as storing a security information for new users to verify their access attempts on the network (col. 9,

Art Unit: 2431

lines 36-55). It would have been obvious to profile new users because the system has yet to analyze their behavioral patterns. This would greatly increase the systems ability to correctly deal with new users while patterns are detected. It is obvious to combine known method which produced predictable results. One of ordinary skill in the art would have been motivated to create a separate profile for new users in order to deal with them efficiently until a pattern of behavior could be established.

With respect to claim 24, McCallum is silent in explicitly teaching an operation-record-storer for storing, according to user, totals related to at least one of the following: number of logins to said computer, operation time that said computer has been operated, or number of days said computer has been operated; and

a first-time-user-judgment mechanism for referencing said operation-record-storer, and determining that a user executing said operation is a first-time user using said computer for the first time when said totals do

not satisfy preset reference values; and wherein said third profile-creator creates a third profile for an operation executed by a user that is determined to be a first-time user by said first-time-user-judgment mechanism; and

said score-calculator uses at least one profile stored in said third profile-storer when said first-time-user-judgment mechanism determines that a user is a first-time user to determine whether said operation is an unauthorized operation.

Sekiguchi teaches an operation-record-storer for storing, according to user, totals related to at least one of the following: number of logins to said computer, operation time that said computer has been operated, or number of days said computer has been

Art Unit: 2431

operated [col. 9, lines 40-42; access restriction information is kept for new users for a predetermined amount of time]; and

a first-time-user-judgment mechanism for referencing said operation-record-storer, and determining that a user executing said operation is a first-time user using said computer for the first time when said totals do not satisfy preset reference values (col. 9, lines 40-41);

and wherein said third profile-creator creates a third profile for an operation executed by a user that is determined to be a first-time user by said first-time-user-judgment mechanism [col. 9, lines 36-38; access restriction applied to new users]; and

said score-calculator uses at least one profile stored in said third profile-storer when said first-time-user-judgment mechanism determines that a user is a first-time user to determine whether said operation is an unauthorized operation (col. 9, line 37; specific security level is used). Sekiguchi teaches these limitations as storing a security information for new users to verify their access attempts on the network (col. 9, lines 36-55). It would have been obvious to profile new users because the system has yet to analyze their behavioral patterns. This would greatly increase the systems ability to correctly deal with new users while patterns are detected. It is obvious to combine known method which produced predictable results. One of ordinary skill in the art would have been motivated to create a separate profile for new users in order to deal with them efficiently until a pattern of behavior could be established.

As per claim 25, McCallum teaches said score-calculator calculates a score by calculating a deviation between said instruction data and data that is stored in said profiles (0070).

As per claim 26, McCallum teaches an operation-stopper for executing a process for stopping said operation when said score value exceeds a reference value (0069).

With respect to claim 27, McCallum teaches the limitation of “a warning-process for executing a process for displaying a warning on an operation screen of said computer, or generating a warning alarm on said computer, when said score exceeds a reference value” (page 6, paragraph 0066) as a sudden access of the database may be inconsistent with the user profile, and may generate an alert that an intrusion or insider misuse is occurring.

With respect to claim 28, McCallam teaches the limitation of “a warning-notification-transmitter for sending a notification warning to an administration server operated by an administrator of said computer that there is a possibility of an unauthorized operation, when said score exceeds a reference value” (page 6, paragraph 0068) as the comparator may examine data at network devices and compare the data to predefined condition. The detection manager may provide an alert or other means of notifying the security server.

With respect to claims 35 and 38, McCallum teaches the limitation of “said login-detector executes detection processing at specified intervals while said computer is in operation” (0079).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

Art Unit: 2431

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431